CLAIMS:

What is claimed is:

1. A method in a data processing system for reporting security situations, comprising the steps of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

2. The method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

3. The method of claim 1, wherein the events include at least one of a web server event, an electronic mail

event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

4. The method of claim 1, further comprising:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

5. The method of claim 1, wherein the target attribute represents one of a computer and a collection of computers.

6. The method of claim 1, wherein the source attribute represents one of a computer and a collection of computers.

7. The method of claim 1, further comprising:

aggregating a subset of the groups into a combined group.

8. A computer program product in a computer readable medium for reporting security events, comprising instructions for:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

9. The computer program product of claim 8, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

10. The computer program product of claim 8, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

11. The computer program product of claim 8, comprising additional instructions for:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

12. The computer program product of claim 8, wherein the target attribute represents one of a computer and a collection of computers.

13. The computer program product of claim 8, wherein the source attribute represents one of a computer and a collection of computers.

14. The computer program product of claim 8, comprising additional instructions for:

aggregating a subset of the groups into a combined group.

15. A data processing system for reporting security events, comprising:

a bus system;

a memory;

a processing unit, wherein the processing unit

includes at least one processor; and

a set of instructions within the memory,

wherein the processing unit executes the set of instructions to perform the acts of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and

calculating severity levels for the groups;

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

16. The data processing system of claim 15, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

17. The data processing system of claim 15, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

18. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

19. The data processing system of claim 15, wherein the target attribute represents one of a computer and a collection of computers.

20. The data processing system of claim 15, wherein the source attribute represents one of a computer and a collection of computers.

21. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

aggregating a subset of the groups into a combined group.